Evan A. Schmutz (3860)
eschmutz@djplaw.com
Jordan K. Cameron (12051)
jcameron@djplaw.com
DURHAM JONES & PINEGAR, P.C.
3301 N Thanksgiving Way, Suite 400
Lehi, Utah 84043
Telephone: (801) 375-6600
Fax: (801) 375-3865

Attorneys for Plaintiff XMission, L.C.

UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

XMISSION, L.C., a Utah company, Plaintiff, vs. CLICKBOOTH.COM, LLC, a Florida limited liability company; DOES 1-40, Defendants.	**XMISSION, L.C.'S MOTION FOR TEMPORARY RESTRAINING ORDER AND REQUEST FOR PRELIMINARY INJUNCTION; MEMORANDUM OF POINTS AND AUTHORITIES** Case No.: 2:15cv00420 DBP Magistrate Judge Dustin B. Pead

TABLE OF CONTENTS

TABLE OF AUTHORITIES

A. **Cases**

B. Statutes and Rules

COMES NOW Plaintiff XMission, L.C. ("XMission"), and hereby moves the Court, pursuant to Fed. R. Civ. P. 65(a) and 65(b) to temporarily restrain and/or preliminarily enjoin Defendant, Clickbooth.com, LLC and its employees, servants, agents, affiliates, successor and/or assigns and all persons acting in concert or participation with any of them from participating in the transmission of commercial e-mails to XMission and/or any of its customers. Plaintiff respectfully requests that Defendant be temporarily restrained pending the Court's hearing and ruling on Plaintiff's motion for preliminary injunction, which may be expedited as appropriate. Plaintiff submits this Motion together with a supporting Memorandum of Points and Authorities setting forth, in detail, the grounds for its Motion.

Statement of Facts

1. XMission was founded in 1993 as Utah's first Internet Service Provider ("ISP"). Decl. of Peter L. Ashdown, ¶ 3 (hereinafter "Ashdown Decl."), filed concurrently herewith.

2. From its early days as a private, Utah ISP, to its current role as a global business Internet provider, XMission has expanded its technical offerings to include sophisticated cloud hosting, web hosting, e-mail service and hosting, collaboration tools, business VoIP phone service, and high speed Internet connectivity solutions including optical Ethernet, copper and fiber. *Id*. at ¶ 4.

3. Throughout its history, XMission has also worked with hundreds of Utah's nonprofit organizations by providing free web hosting services, and by sponsoring a variety of community-based events and facilities. *Id*. at ¶ 5.

4. XMission is a widely known and well-recognized ISP in Utah. *Id*. at ¶ 6.

5. In cooperation with Salt Lake City government, XMission provides free WiFi to the downtown Salt Lake City metropolitan area. *Id*. at ¶ 7.

6. XMission currently has 38 employees. *Id*. at ¶ 8.

7. XMission owns all the servers, routers, and switches on its network through which it hosts and provides its Internet access services for its customers. *Id*. at ¶ 9.

8. XMission has an expansive network and infrastructure, which it has had to consistently update, upgrade and augment in order to combat ongoing SPAM problems. *Id*. at ¶ 10.

9. XMission is the sole owner of all its hardware, and has complete and uninhibited access to, and sole physical control over, the hardware. *Id*. at ¶ 11.

10. XMission provides Internet access services to both commercial and residential customers. *Id*. at ¶ 12.

11. The e-mail accounts hosted and served by XMission include e-mail accounts owned by third-party customers of XMission, e-mail accounts owned by employees and/or customers of XMission's third-party customers, e-mail accounts owned by employees of XMission, and also e-mail accounts owned by XMission itself. *Id*. at ¶ 13.

12. XMission's network consists of approximately 65,000 main accounts with 12,400 billable entities. *Id*. at ¶ 14.

13. From early January, 2015 through the date of the Complaint filed in this matter on June 11, 2015, XMission had received approximately 105,966 SPAM e-mails that it has accounted for, that were sent and/or initiated by Clickbooth which have adversely affected XMission, and which have contributed to an overall SPAM problem. *Id*. at ¶¶ 33-50.

14. Each of the e-mails is a commercial message and contains commercial content. *Id*. at ¶ 44.

15. Each of the e-mails was received by XMission on its mail servers located in Utah. *Id*. at ¶ 45.

16. Each of the e-mails in question contains redirect links (i.e. including clickbooth.com and clickbooth.net) through which Clickbooth is identified as a responsible transmitting party. *Id*. at ¶ 34.

17. The SPAM e-mails received through the date of the Complaint on June 11, 2015, resulted in 9,372 customer spam complaints/reports to XMission. *Id*. at ¶ 49.

18. Approximately 962 of the e-mails received through June 11, 2015, contained header information including sender IP addresses that either do not belong to the identified sender domain, were not recognized by a legitimate Domain Name Service as belonging to the identified sender domain, and/or do not identify the actual source of the e-mail. *See id*. at ¶¶ 58-60.

19. Approximately 18,884 of the e-mails received through June 11, 2015, contain generic from names and originated from privacy-protected sender domains. *Id*. at ¶¶ 61-65.

20. Approximately 416 e-mails received through June 11, 2015, included a "from" name that was deceptive in that it created the impression that the e-mail was from a party with whom the recipient had a prior, transactional relationship. *See id*. at ¶¶ 66-67.

21. Approximately 100,612 of the e-mails received through June 11, 2015 originated from sender domains registered with an ICANN compliant domain registrar who maintains an

anti-spam policy, and these sender domains served no purpose other than to engage in activities that violate the anti-spam policies. *See id*. at ¶¶ 68-89.

22. Specifically, e-mails were sent from sender domains registered with 1&1 Internet AG; BigRock Solutions, Ltd.; DomainDiscover; DomainSite, Inc.; Dynadot, LLC; Gandi SAS; GoDaddy.com; Internet.bs Corp.; Name.com, Inc.; Namesilo, LLC; PDR Ltd. d/b/a PublicDomainRegistry.com; Register.com; and, Wild West Domains, LLC. *See id*. at ¶¶ 73-86.

23. None of the sender domains registered with the aforementioned domain registrars appear to resolve to any legitimate website or have any legitimate function other than mass e-mail marketing, which violates the anti-spam policies in question. *See id*. at ¶¶ 87-88.

24. In fact, each sender domain was used to transmit SPAM e-mail messages to XMission. *Id*. at ¶ 88.

25. XMission's Terms of Service provide that "XMission may take action on [customers'] behalf to mitigate SPAM and [customers] grant to XMission the authority and right to opt-out and/or unsubscribe from receiving any and all SPAM emails, sent by any party to your email address(es)." *Id*. at ¶ 41.

26. XMission has attempted to click on available unsubscribe links in each of the received e-mails, but such does not appear to have stopped commercial e-mails. *Id*. at ¶ 42.

27. Throughout its business history, XMission has expended well in excess of $3,000,000 in hardware acquisition, maintenance and related expenses to increase capacity to deal with increased SPAM and related harm, SPAM filtering expenses, and employee time in dealing with problems caused by its receipt of SPAM generally. *Id*. at ¶ 15.

28. XMission expends approximately $100,000 to $200,000 per year in dealing with SPAM related issues and associated employee time, exclusive of attorney fees. *Id*. at ¶ 16.

29. XMission has two full-time employees whose primary responsibilities are to deal with SPAM related issues, including, adjust filtering, responding to customer complaints, addressing blacklist issues, and acting as first responders to data security breaches, and hardware issues caused by SPAM. *Id*. at ¶ 17.

30. XMission also employs 15 other technicians who dedicate at least part of their time to dealing with the aforementioned SPAM issues. *Id*. at ¶ 18.

31. XMission currently has 13 servers dedicated specifically to process SPAM. Those servers could be dedicated to providing XMission's internet access services if it were not for the SPAM. XMission has had more total spam-mitigation servers over its history. *Id*. at ¶ 19.

32. Approximately 13% of all general technical support staff time and 39% of mail administrative time is dedicated to dealing with SPAM related issues. *Id*. at ¶ 20.

33. Daily between 40% and 85% of the e-mail messages that XMission receives on its system are SPAM e-mails, of which the subject e-mails are a part. Historically XMission estimates an average spam level of 60% of all e-mail hitting XMission systems. *Id*. at ¶ 21.

34. The percentage of SPAM e-mails would be significantly higher if not for all the precautions that XMission has taken, including subscribing to leading anti-spam services, including blacklists such as URIBL and Spamhaus, in addition to creating customized and proprietary filtering rules and e-mail server configurations utilizing tools such as SpamAssassin. *Id*. at ¶ 22.

35. For each e-mail at issue in the lawsuit, XMission had to expend man hours and work to identify the source, to examine the transmission information, to examine and analyze the header information, to take efforts to determine how and why the specific e-mails were able to circumvent and/or bypass preliminary filtering techniques, and to ultimately attempt to make the e-mails stop. *Id*. at ¶ 23.

36. On June 12, 2015, XMission filed a Complaint against Clickbooth for violations of 15 U.S.C. § 7701 et seq., otherwise known as the CAN-SPAM Act. *Id*. at ¶ 44.

37. The e-mails are continuing on a daily basis, as of the date of this Motion, and XMission continues to receive customer complaints associated with the e-mails. *Id*. at ¶¶ 50-51.

38. One of XMission's competitive advantages is that is has historically been able to offer an Internet access service with greatly reduced SPAM traffic. *Id*. at ¶ 52.

39. However, in recent years, as the number of SPAM e-mails has increased, the number of e-mails that are bypassing XMission's SPAM filtering techniques has continued to grow. *Id*. at ¶ 53.

40. These e-mails include the e-mails at issue in this lawsuit. *Id*. at ¶ 54.

41. In addition to specific customer complaints related to the Clickbooth e-mails, XMission's reputation and competitive advantage has been harmed, and will continue to be harmed, because customers have taken notice of the growing number of SPAM e-mails reaching their inboxes, and have expressed dissatisfaction with XMission and doubt as to XMission's ability to offer a SPAM free service. *Id*. at ¶ 55.

42. If the e-mailing is allowed to persist, it will result in possible loss of customers, and a significant, and likely irreparable, damage to XMission's reputation and competitive advantage in the market place. *Id*. at ¶ 56.

Argument

I. LEGAL AUTHORITY

A plaintiff seeking a preliminary injunction must establish "that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest. *Winter v. Natural Resources Defense Council, Inc.*, 129 S. Ct. 365, 374 (2008); *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006); *Dominion Video Satellite, Inc. v. Echostar Satellite Corp.*, 356 F.3d 1256, 1260 (10th Cir. 2004). The "decision whether to grant or deny injunctive relief rests within the equitable discretion of the district courts, and that such discretion must be exercised consistent with traditional principles of equity . . . ." *eBay Inc.* 547 U.S. at 394.

II. XMISSION IS LIKELY TO SUCCEED ON THE MERITS OF ITS CAN-SPAM ACTION.

A. XMission likely has standing to pursue CAN-SPAM claims.

The CAN-SPAM Act states that a provider of Internet access service that is adversely affected by unlawful commercial email may bring a civil action in any district court of the United States with jurisdiction over the defendant. *See* 15 U.S.C. § 7706(g)(1). Here, XMission has standing to bring actions under CAN-SPAM because (1) it is a *bona fide* Internet access service, and (2) it is adversely affected by unlawful commercial emails, including the emails in question.

1. XMission is a *bona fide* Internet access service.

The CAN-SPAM Act defines Internet access service as "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services." *See* 15 U.S.C. § 7702(11) citing 47 U.S.C. § 231(e)(4). The Ninth Circuit, in *Gordon v. Virtumundo*, further limited standing to "*bona fide*" Internet Access Services, which it defined by citing to the Congressional Record in stating "[W]e intend that Internet access service providers provide actual Internet access service to customers."[1] *See Gordon*, 575 F.3d 1040, 1050 (9th Cir. 2009) (citing 150 Cong. Rec. E72-02). Courts have extended the definition of Internet access services to "include[ ] traditional [ISPs], any email provider, and even most website owners." *MySpace, Inc. v. The Globe.com, Inc.*, No. 06-3391, 2007 WL 1686966, at *3 (C.D.Cal. Feb.27, 2007) (lodged herewith as Exhibit 22); *see also Facebook, Inc. v. ConnectU LLC*, 489 F. Supp. 2d 1087, 1094 (N.D.Cal. 2007) (lodged herewith as Exhibit 23).

Here, XMission is a *bona fide* Internet Access Service. *See supra* Statement of Facts ¶¶ 1-12. Specifically, XMission offers sophisticated cloud hosting, web hosting, e-mail service and hosting, collaboration tools, business VoIP phone service, and high speed internet connectivity solutions including optical Ethernet, copper and fiber. *Id.*, Fact 2. XMission is widely

[1] The plaintiff in *Gordon* did not qualify as an Internet Access Service despite providing email accounts because "Gordon [was] a registrant of a domain name, which he, through Omni, hosts on leased server space. He neither has physical control over nor access to the hardware, which GoDaddy owns, houses, maintains, and configures . . . . Gordon's service appears to be limited to using his "Plesk" control panel, which he accesses via an ordinary Internet connection through an ISP, to set up e-mail accounts and log-in passwords and to execute other administrative tasks. Verizon enables his online access. GoDaddy provides the service that enables ordinary consumers to create e-mail accounts, register domain names, and build personalized web pages. Gordon has simply utilized that service for himself and on behalf of others." *Gordon*, 575 F.3d at 1052.

recognized as a legitimate Internet provider in and for the Salt Lake City metropolitan area, and worked with hundreds of Utah's nonprofit organizations by providing free web hosting services, and by sponsoring a variety of community-based events and facilities, including offering free WiFi to the Salt Lake City metropolitan area. *See id*., Facts 3-5. XMission owns all the servers, routers, and switches on its network through which it hosts and provides its internet access services for its customers. *Id*., Fact 7. XMission has sole ownership of all the hardware, complete and uninhibited access to the hardware, and sole physical control over the hardware. *Id*., Fact 9. Importantly, XMission was founded in 1993, twenty years before the CAN-SPAM Act was passed in to law. *See id*., Fact 1. Unlike Gordon, who attempted to establish various e-mail accounts to take advantage of the CAN-SPAM Act (*see Gordon*, 575 F.3d at 1052), XMission existed long before the Act was ever contemplated.

For the reasons set forth above, XMission is a bona fide Internet access service and qualifies for standing to assert actions under the CAN-SPAM Act.

2. XMission is adversely affected by unlawful commercial emails, including the emails in question.

As set forth in *Gordon*, the harm suffered by an Internet Access Service in order to establish standing under the "adverse affect" requirement of the CAN-SPAM Act "need not be significant in the sense that it is grave or serious, [but] must be of significance to a *bona fide* IAS provider-something beyond the mere annoyance of spam . . . ." *Gordon*, 575 F.3d at 1053-54. The court further explained that "[i]n most cases, evidence of some combination of operational or technical impairments and related financial costs attributable to unwanted commercial e-mail would suffice." *Id*. at 1054.

Here, XMission has experienced, and continues to experience on a daily basis, significant

operational and technical impairments with related financial costs. *See*, *supra*, Facts 27-35, 38-42. Throughout its business history, XMission has expended well in excess of $3,000,000 in hardware acquisition, maintenance and related expenses to increase capacity to deal with increased SPAM and related harm, SPAM filtering expenses, and employee time in dealing with problems caused by its receipt of SPAM generally. *Id*., Fact 27. XMission expends approximately $100,000 to $200,000 per year in dealing with SPAM related issues and associated employee time, exclusive of attorney fees. *Id*., Fact 28. XMission has two full-time employees whose primary responsibilities are to deal with SPAM related issues, including, adjust filtering, responding to customer complaints, addressing blacklist issues, and acting as first responders to data security breaches, and hardware issues caused by SPAM. *Id*., Fact 29. XMission also employs 15 other technicians who dedicate at least part of their time to dealing with the aforementioned SPAM issues. *Id*., Fact 30. XMission has to dedicate 13 serves to specifically process SPAM. *Id*., Fact 31. Those servers could be dedicated to providing other Internet access services if it were not for the SPAM. *Id*. Approximately 13% of all general technical support staff time and 39% of mail administrative time is spent dealing with SPAM related issues. *Id*., Fact 32.

The *Gordon* standard for standing does not require that a plaintiff prove that the emails at issue adversely affect the plaintiff, rather, that "[t]he e-mails at issue in a particular case . . . contribute to a larger, collective spam problem." *See Gordon*, 575 P.3d at 1054. On average, approximately 60% of the email messages that XMission receives on its system are unlawful commercial emails, of which the subject emails are a part. *See*, *supra*, Fact 33. This number would be significantly higher if not for all the precautions that XMission has taken. *Id*., Fact 34.

Though not required to prove standing, XMission can demonstrate that the Clickbooth e-mails adversely affected it. In 2012, the Northern District of California, in *Facebook v. Power Ventures, In*c. ruled on a summary judgment motion that addressed standing. *See* 844 F. Supp. 2d 1025 (N. D. Cal. 2012) (lodged herewith as Exhibit 24). In that decision, the court provided a very helpful analysis of the *Gordon* standard for standing.

There, the court determined that Facebook's receipt and analysis of approximately 60,000 messages constituted an adverse effect. *Id*. at 1032. It is worth noting that, around the time of the *Power Ventures* case, Facebook's network consisted of 901 million users and Facebook had over 3,000 employees. *See* Facebook Newsroom, 2012 (lodged herewith as Exhibit 25). In that case, Facebook outlined its harm, with respect to the emails in question, as having to spend time and effort determining the source of the emails, and taking steps to get the emails to stop. *See Power Ventures*, 844 F. Supp. 2d at 1031. The court held that Facebook did demonstrate an adverse effect, and that such was especially true because there were a documented 60,000 messages, and "the cost of responding to such a volume of spamming cannot be categorized as 'negligible.'" *Id*. at 1032.

In this case, XMission network consists of approximately 65,000 users, XMission has 38 employees, and there are 105,966 e-mails at issue. *See*, *supra*, Facts 6, 12-13. Accordingly, the subject emails created a significantly greater burden for XMission than the 60,000 e-mails received by Facebook's 901 million users and over 3,000 employees. Similar to Facebook, for each e-mail, XMission has expended man hours and work to identify the source, to examine the transmission information, to examine and analyze the header information, to take efforts to determine how and why the specific e-mails were able to circumvent and/or bypass preliminary

filtering techniques, and to ultimately attempt to make the e-mails stop. *See*, *supra*, Fact 35. Perhaps more importantly, XMission has received 9,372 customer complaints associated with Clickbooth e-mails. *Id*., Fact 17.

As stated in *Power Ventures*, XMission has standing to pursue CAN-SPAM claims against Clickbooth because the documented efforts related to XMission's attempts to identify and block the subject emails cannot be categorized as negligible and therefore confer standing. *See Power Ventures*, 844 F. Supp. 2d at 1032. Of course, the Court need not go to such a lengthy analysis to determine that XMission has standing where, as stated in *Gordon*,

> the threshold of standing should not pose a high bar for the legitimate service operations contemplated by Congress. In some civil actions—where, for example, well-recognized ISPs or plainly legitimate Internet access service providers file suit—adequate harm might be presumed because any reasonable person would agree that such entities dedicate considerable resources to and incur significant financial costs in dealing with spam.

Gordon, 575 F. 3d at 1055 (citing S.Rep. No. 108-102, at 2-3 (recounting reports by America Online, Microsoft, and Earthlink regarding the effects of increasing volumes of spam)). There can be no dispute that XMission is a well-recognized and plainly legitimate Internet service provider for which harm is presumed.

B. Clickbooth is likely an "Initiator."

E-mail advertising typically involves three separate actors plus the consumer. The "publisher" who distributes/ transmits the commercial e-mails, the "advertiser" who is the party seeking to generate awareness for and sales of its products and services, and the "marketing network" (in this case, Clickbooth) who has relationships with publishers and advertisers and facilitates the e-mail marketing for the advertisers with the assistance of the publishers. The CAN-SPAM Act places these three actors into two separate categories: "Senders" and

"Initiators." See 15 U.S.C. § 7702(9), (16). Importantly, the CAN-SPAM Act recognizes that there can be multiple "Initiators" for each e-mail (see 15 U.S.C. § 7702(9)), and assigns independent liability for each "Sender" and each "Initiator" when certain criteria are satisfied. See 15 U.S.C. § 7704.

Liability under the CAN-SPAM Act attaches to advertisers, publishers and marketing networks (i.e. "Senders" and "Initiators") who "procured" the commercial e-mails in question. 15 U.S.C. § 7702(9). Congress explained that, "[m]ore than one person may be considered to have initiated a message. Thus, if one company hires another to handle the tasks of composing, addressing, and coordinating the sending of a marketing appeal, both companies could be considered to have initiated the message–one for procuring the origination of the message; the other for actually originating it." Senate Report No. 108-102, 2003 WL 21680759, 14, 2004 U.S.C.C.A.N. 2348, 2360 (July 16, 2003) (lodged herewith as Exhibit 26).

When an Internet access service provider, such as XMission, is seeking relief from violations of the CAN-SPAM Act, a party "procures" the origination or transmission of commercial electronic mail when it "intentionally pay[s] or provide[s] other consideration to, or induce[s], another person to initiate such a message on one's behalf with actual knowledge, or by consciously avoiding knowing, whether such person is engaging, or will engage, in a pattern or practice that violates this chapter" 15 U.S.C. §§ 7702(12), 7706(g)(2). "The intent of" this definition of procure "is to make a company responsible for e-mail messages that it hires a third party to send, unless that third party engages in renegade behavior that the hiring company did not know about. However, the hiring company cannot avoid responsibility by purposefully remaining ignorant of the third party's practices. The 'consciously avoids knowing' portion of

this definition is meant to impose a responsibility on a company hiring an e-mail marketer to inquire and confirm that the marketer intends to comply with the requirements of this Act." Senate Report No. 108-102, at 2360.

To the extent Clickbooth did not directly transmit the commercial e-mail messages, it certainly procured the e-mail messages as such is defined in the Act. One example of a procurer, which appears to apply here, is a business that provides the method and process through which companies are able to market their goods, services, and/or webpages through mass e-mail marketing, whose e-mails are usually sent by third party affiliates. To protect itself from suits, often an alleged procurer will claim ignorance of violations under the Act. Clickbooth can make no such claim.

Prior to this lawsuit, various other parties have either sued Clickbooth or put Clickbooth on notice of its abusive and unlawful spamming practices. For example, in 2008, Asis Internet Services sued Clickbooth for repeatedly sending thousands of commercial e-mails that contained materially false or misleading header information, including but not limited to: (i) misleading subject lines that materially misrepresented the actual content and subject matter of the message; and (ii) misleading and false sender information that made it impossible, without a subpoena, to identify the true registrant for the sender. *See Asis Internet Services v. Active Response Group, Inc. et al.,* Case No. C-07-6211 (N.D. Cal. 2008) (Cmplt. lodged herewith as Exhibit 27). In 2012, ZooBuh, Inc. notified Clickbooth that Clickbooth was in violation of the CAN-SPAM Act by continuously initiating commercial e-mails that contained materially false or deceptively misleading header information, similar to the header information that formed the basis for Asis' 2008 action. Clickbooth responded by filing a declaratory action. *See Clickbooth.com, LLC. v.*

Zoobuh, Inc., Case No. 8:12-cv-01021 (M D. Fla. 2012) (Clickbooth Cmplt. lodged herewith as Exhibit 28). Importantly, Clickbooth's Complaint outlines the various claims asserted by ZooBuh and clearly identifies that, as of 2012, Clickbooth was on notice of its abusive e-mail practices that were alleged to violate the CAN-SPAM Act.

ZooBuh also sued Clickbooth and further put Clickbooth on notice of the manner in which its e-mails were misleading, including specifically, that the Clickbooth e-mails contained header information with: (i) illegitimate sender IP addresses; (ii) information that was obtained by means of false or fraudulent pretenses (e.g. obtaining sender domain names and email addresses under an agreement not to use the domains and addresses for sending unsolicited commercial email); (iii) altered or concealed information that impaired the ability of the party processing the message to identify or respond to the transmitting party; and (iv); "from" lines that did not accurately identify the sender of the message and that were accompanied by originating email addresses that were cloaked or privacy protected, thereby impeding the recipient from identifying the initiating party. *See ZooBuh, Inc. v. Clickbooth.com, LLC*, Case No. 2:12cv00455 (D. Utah 2012) (Cmplt. lodged herewith as Exhibit 29).

In addition to the aforementioned action regarding abusive e-mail practices, other entities and regulatory authorities have sued Clickbooth and Clickbooth has confessed to judgment for its fraudulent and misleading marketing practices. For example, in 2009, Clickbooth was a defendant in a class action lawsuit that alleged, *inter alia*, that Clickbooth produced false and misleading advertisements with the purpose of driving consumer traffic to advertiser's websites. *See Chamberlain v. Integraclick, Inc., et al.*, Case No. 2009-CA-4695 (C. D. Fla. 2009) (Cmplt. lodged herewith as Exhibit 30). Specifically, its advertisements failed to reveal

material facts regarding product offerings, relied on false affiliations with third party entities, and used other misleading tactics to mislead consumers. *Id*. at ¶¶ 14-16; 22-26; 31-32; 37-39; 67-73. In 2012, Clickbooth stipulated to entry of judgment against it and an order of permanent injunction in *Federal Trade Commission v. Clickbooth, et, al.* Case No. 12-cv-9087 (N. D. Ill. 2012) (Stipulated Final Judgment lodged herewith as Exhibit 31). The stipulation prohibited Clickbooth from continuing to make certain misrepresentations in its marketing materials for third parties. *Id*. at pp. 8-9. Clickbooth also stipulated to entry of judgment in the amount of $2,000,000 as a sanction for its misleading marketing practices. *Id*. at p. 18. In 2012, in response to being investigated by Florida's Attorney General for deceptive or unfair trade practices, Clickbooth entered into an Assurance of Voluntary Compliance. *See In the Matter of: Clickbooth.com, LLC d/b/a EOGC Enterprises and IntegraClick,* Case No. L10-3-1156 (Assurance of Voluntary Compliance lodged herewith as Exhibit 32). Pursuant to the Assurance of Voluntary Compliance, Clickbooth agreed to change its deceptive or unfair trade practices and pay $500,000.00.

In summary, Clickbooth has a significant history of engaging in false and misleading marketing practices across many marketing platforms. The e-mails in this case are no exception. Through the various lawsuits and demands identified above, Clickbooth has had repeated notice that its marketing practices are suspect and violate the law. However, Clickbooth appears to have done nothing to modify its practices, and the same abusive practices that gave rise to the e-mail lawsuits identified herein are what give rise to the instant lawsuit.

Even if Clickbooth did not have actual knowledge that it or the third party entities initiating the commercial e-mails on Clickbooth's behalf were violating the CAN-SPAM Act,

Clickbooth would still likely be an "Initiator" by consciously avoiding such knowledge. *See* 15 U.S.C. § 7706(g)(12). To make such determination, the Court must decide if proper steps were taken to "inquire and confirm" that the parties transmitting the commercial e-mails would comply with the law. *See* Senate Report No. 108-102, at 2360.

In *Asis v. Optin Global*, the court stated that that the "procure" element can be satisfied where the defendant decides not to learn that its affiliates were violating the CAN-SPAM Act. *See* 2008 WL 1902217 *18 (N.D. Cal. April 28, 2008) (lodged herewith as Exhibit 33), affirmed by *ASIS Internet Srvcs. v. Azoogle.com, Inc.*, 357 Fed. App. 112 (9th Cir. Dec. 2, 2009). As set forth herein, the commercial emails in question are so full of patent and readily identifiable violations of the CAN-SPAM Act (of the exact same type of which Clickbooth has been notified on multiple occasions) that, unless Clickbooth decided not to learn of the violations, it would undoubtedly learn of the violations and the non-compliance of its affiliates. The *Asis* Court also stated that "[t]he defendant need not have specific knowledge of the identity of the individual sending the spam to meet the 'conscious avoidance' standard." *Id.* Furthermore, the *Asis* decision implied that the "procure" element could be satisfied in circumstances where, had the defendant investigated its affiliates (or the third parties hired by its affiliates), it would have learned that the e-mailers engaged in CAN-SPAM violations. *See id*. at *19.

Because the commercial e-mails in question are full of patent and readily identifiable CAN-SPAM violations, it is likely that Clickbooth failed to take the proper steps to inquire and confirm that the third-party sending the commercial e-mails on behalf of Clickbooth were abiding by the law. In other words, it is likely that Clickbooth consciously avoided such knowledge and therefore initiated the commercial e-mails that violate the CAN-SPAM Act.

C. The E-mails contain significant CAN-SPAM violations.

The CAN-SPAM Act makes it unlawful for any person to initiate the transmission of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. *See* 15 U.S.C. § 7704(a)(1).

1. Many of the e-mails in question violate 15 U.S.C. § 7704(a)(1).

Header information is materially false or materially misleading under Section 7704(a)(1) where it includes an inaccurate transmission IP address. In other words, the transmitting party represented that the e-mail was being sent from a specific domain, when in fact, the IP address used to actually transmit the e-mail does not match the represented sender domain or does not resolve to any legitimate domain. *See*, *supra*, Fact 18. Under these circumstances, the header information is false on its face. Here, 962 e-mails were transmitted with header information including sender IP address that did not match the represented sender domain or did not resolve to any legitimate domain and were therefore false on their face. *See id*. Accordingly, these e-mails violate 15 U.S.C. § 7704(a)(1).

Header information is materially false or materially misleading under Section 7704(a)(1) where the "from" name is generic and the sender domain is privacy protected. *See ZooBuh v. Better Broadcasting*, 2013 WL 2407669, *6 (D. Utah, May 31, 2013) (lodged herewith as Exhibit 34) ("Accordingly, where an email contains a generic 'from' name and is sent from a privacy-protected domain name, such that the recipient cannot identify the sender from the 'from' name or the publicly available WHOIS information, such is 'materially misleading' and is a violation . . . ."). Here, 18,884 e-mails contained a generic "from" line and originated from a

privacy protected domain. *See*, *supra*, Fact 19. Accordingly, these e-mails violate 15 U.S.C. § 7704(a)(1); *see also ZooBuh* at *6.

Header information is materially false or materially misleading under Section 7704(a)(1) where the "from" name is misleading in that it is designed to induce the recipient to open an e-mail under a false pretense. "People have a right to assume that fraudulent advertising traps will not be laid to ensnare them. 'Laws are made to protect the trusting as well as the suspicious.'" *Donaldson v. Read Magazine, Inc.*, 333 U.S. 178, 189 (1948) (citing *Federal Trade Comm'n v. Standard Education Society*, 302 U.S. 112, 116 (1937)). E-mails containing "from" lines such as "Refinance Approvals", "Credit Alert", "Approval Department", "LoanApproval Notice", "Loan Manager", and "Score update", create the impression that a company with whom the recipient has an actual and ongoing transactional relationship is attempting to communicate with them regarding that relationship. However, the e-mails are advertisements intended to direct the recipient to a website through which they may purchase a product or service. Therefore, 416 of the e-mails in question contain "From" lines that are materially misleading and have the purpose of inducing the recipient to view the e-mail in violation of 15 U.S.C. § 7704(a)(1). *See*, *supra*, Fact 20.

2. Many of the e-mails in question violate 15 U.S.C. § 7704(a)(1)(A).

In *ZooBuh*, the Court determined that an e-mail that originated from a sender domain registered with an ICANN compliant domain registrar who maintains an anti-spam policy, violates the law regardless of whether the e-mail contains a header that is technically accurate. *See ZooBuh* at *6-7. The Court reasoned that:

> in order to obtain the domain names used to send the e-mails in question, the Defendants represented to the domain registrars that the domain names would not be used for SPAM

> purposes. However, the domain names were intended to be used, and were used, for SPAM purposes. Consequently, the Defendants obtained the sender domains . . . under false and fraudulent pretenses . . . .

Id. To constitute a violation of 7704 (a)(1)(A) as set forth in *Better Broadcasting*, there are three necessary elements: 1) the sender domain was registered with an ICANN compliant domain registrar; 2) the registrar maintains an anti-spam policy; and, 3) the domain was registered for a purpose that violates that registrar's policy. *See id*.

Here, 100,612 of the Clickbooth e-mails were sent from domains registered with ICANN compliant domain registrars, each of whom maintains anti-spam policies. *See*, *supra*, Fact 21. In satisfaction of the third element established by *ZooBuh*, a review of sender domain names, and the weight of the evidence, indicates that such were registered for the sole purpose of advertising and/or sending bulk e-mail campaigns despite the agreement by the registrar not to engage in such activities. *See id*., Facts 21-24.

III. CLICKBOOTH'S CONTINUED E-MAILING WILL CAUSE IRREPARABLE HARM TO XMISSION.

The anticipated harm to XMission if an injunction does not enter is not of an economic nature and therefore, is considered irreparable for purposes of an injunction. *See Heideman v. S. Salt Lake City*, 348 F.3d 1182, 1189 (10th Cir. 2003). The anticipated harm is in the form of damage to goodwill, loss of customers, and loss of XMission's competitive position based on its historic ability to protect customers from SPAM, which is now in jeopardy as the result of Clickbooth's sophisticated spamming practices which allow their e-mails to bypass XMission's SPAM filtering efforts. *See Dominion Video v. Echostar Sat. Corp.*, 356 F. 3d 1256, 1263 (10th Cir. 2004). (identifying "the following as factors supporting irreparable harm determinations:

inability to calculate damages, harm to goodwill, diminishment of competitive positions in marketplace . . . .")

XMission faces an immediate and incalculable threat of harm to its reputation through Clickbooth's actions. Each time Clickbooth e-mails are received, customers complain of those e-mails. *See*, *supra*, Fact 37. In the two days preceding the filing of its Complaint against Clickbooth, XMission received, and accounted for, 1,882 Clickbooth e-mails and received 61 customer complaints related to those e-mails. *See* Ashdown Decl. at ¶ 51. In total, XMission has received 9,372 customer complaints arising as the result of the Clickbooth e-mails. *See*, *supra*, Fact 17. Of course, with each passing day, the number of customer complaints will increase, and XMission's goodwill and reputation will continue to be harmed as the result. *Id.*, Facts 37-42. Further, if the e-mailing is allowed to persist, it will result in an anticipated loss of customers, and a significant, and likely irreparable, damage to XMission's reputation and competitive advantage in the market place. *Id.*, Fact 42.

Moreover, the CAN-SPAM Act itself recognizes the irreparable nature of harm caused to an Internet service provider by its receipt of SPAM e-mails. In the Congressional findings set forth in the CAN-SPAM Act, Congress identified various, significant facts relating to the irreparable harm associated with SPAM e-mail. Specifically:

> (2) The convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail. . . .
> (4) The receipt of a large number of unwanted messages also decreases the convenience of electronic mail and creates a risk that wanted electronic mail messages, both commercial and noncommercial, will be lost, overlooked, or discarded amidst the larger volume of unwanted messages, thus reducing the reliability and usefulness of electronic mail to the recipient.

15 U.S.C. § 7701(a)(2), (4).

In addition to the threatened loss of goodwill and harm to reputation, if an injunction does not enter, XMission faces a loss of convenience and efficiency of its service to its customers and an increased risk that legitimate e-mail messages will be lost or overlooked, thereby reducing the reliability and usefulness of XMission's service. This damage is not quantifiable, but is substantial. Together, the aforementioned, threatened harm, is precisely the type of harm that is fundamentally irreparable and for which a proper calculation cannot be made.

IV. THE BALANCE OF HARM WEIGHS IN FAVOR OF XMISSION AS AN INTERNET ACCESS SERVICE RESPONSIBLE FOR PROTECTING ITS CUSTOMERS FROM ABUSIVE SPAM PRACTICES.

Under the CAN-SPAM Act, an individual e-mail recipient does not have a private right of action. *See* 15 U.S.C. § 7706. Instead, an individual can attempt to opt-out from receiving e-mails. To that point, the CAN-SPAM Act makes it unlawful for an e-mailer to continue to send commercial e-mails more than 10 business days after the receipt of a request to unsubscribe. *See* 15 U.S.C. § 7704(a)(4).

Pursuant to its Terms of Service, which provides that "XMission may take action on [customer's] behalf to mitigate SPAM and [customers] grant to XMission the authority and right to opt-out and/or unsubscribe from receiving any and all SPAM emails, sent by any party to your email address(es)", XMission has attempted to click on available unsubscribe links in each of the received e-mails, but with no apparent effect. *See*, *supra*, Facts 25-26. Therefore, a question exists as to what, if any, recourse, an individual has when opt-out requests are ineffective.

The CAN-SPAM Act created a private right of action for a limited group of qualified entities, including importantly, providers of an Internet access service. *See* 15 U.S.C. § 7706(g). As a *bona fide* provider of an Internet access service, XMission stands as the only buffer, both

legally and technologically, between Clickbooth's SPAM e-mails and the intended recipients. Although XMission has done all it can to technologically combat abusive spamming practices (*see*, *supra*, Facts 25-26, 34) Clickbooth has successfully circumvented Clickbooth's technological defenses and has consistently places thousands of e-mails in XMission customer's inboxes, which it has no right to do.

Without their own legal recourse, the complaining customers have no choice but to rely on XMission to protect their individual interests, which includes, the protection from abusive SPAM practices. To date, XMission has received 9,372 customer complaints related to the Clickbooth e-mails. *See id.*, Fact 17. The number of complaints continues to increase on a daily basis. The e-mails are clearly not wanted. Pursuant to the CAN-SPAM Act, the recipients have a right to decline to receive additional e-mails. *See* 15 U.S.C. §§ 7701(b)(3), 7704(a)(4).

Certainly where the intended XMission recipients have no desire to continue to receive the Clickbooth e-mails, and XMission, as the Internet access service who suffers the direct adverse effect from its receipt of thousands of e-mails, desires to stop the e-mail permanently, Clickbooth has no right to continue to send them, and will suffer no legally recognizable harm if an injunction enters. On the other hand, XMission will continue to suffer significant and irreparable harm, as described more fully in Section III if an injunction does not enter. Therefore, the balance of harm favors XMission's efforts to stop unwanted e-mails and stand as a buffer between the responsible party and the intended recipients through an injunction.

V. PUBLIC INTEREST FAVORS THE PREVENTON OF ABUSIVE SPAM PRACTICES AND THE RIGHTS OF AN INTERNET ACCESS SERVICE TO PROTECT ITS CUSTOMERS' INTERESTS.

Regarding public policy, in the Congressional findings set forth in the CAN-SPAM Act, Congress determined that: "(1) there is a substantial government interest in regulation of commercial electronic mail on a nationwide basis; . . . [and] (3) recipients of commercial electronic mail have a right to decline to receive additional commercial electronic mail from the same source." 15 U.S.C. § 7701(b). As set forth above in Sections III and IV, to further its customers' interest and, consistent with its Terms of Service, XMission has attempted to opt-out on behalf of its customers from the Clickbooth e-mails without success. *See, supra*, Facts 25-26.

Without their own legal recourse, the complaining customers have no choice but to rely on XMission to protect their individual interest, which include protection from abusive SPAM practices. Therefore, public interest significantly favors XMission's efforts to stop unwanted e-mails and stand as a buffer between the responsible party and the intended recipients through an injunction.

As with the balance of harm, where the intended XMission recipients have no desire to continue to receive the Clickbooth e-mails, and XMission, Internet access service who suffers the direct adverse effect from its receipt of thousands of e-mails, desires to stop the e-mail permanently, there is no public interest that would contravene the entry of an injunction.

VI. NO BOND SHOULD BE REQUIRED.

Because Defendants have no right to continue to transmit commercial e-mails once the recipients have expressed a desire to unsubscribe (*see* 15 U.S.C. § 7704(a)(4)), and because XMission is vested with the authority to opt-out on behalf of its customers (*see, supra,* Facts 25-

26), which it has unsuccessfully attempted to do, this injunction will preserve the parties' rights as they presently exist and establish a status quo for the pendency of this litigation. Therefore, XMission respectfully submits that no bond is necessary in this case.

VII. XMISSION RESPECTFULLY REQUESTS EXPEDIENCY.

Because Defendant continues to transmit a high number of e-mails to XMission's customers, despite XMission's attempts to opt-out therefrom, and because the e-mails continue to give rise to customer complaints, XMission respectfully requests that the Court expedite its consideration of XMission's request for a temporary restraining order and also expedite the hearing and briefing schedule for XMission's motion for preliminary injunction.

Conclusion

Based on the foregoing, XMission is likely to succeed on the merits of its case, XMission is likely to suffer irreparable harm in the absence of preliminary relief, the balance of equities tips in XMission's favor, and the proposed injunction is in the public interest. Therefore, this Court should enter a Temporary Restraining Order and Preliminary Injunction until the final resolution of this case.

DATED this 12th day of June, 2015.

DURHAM JONES & PINEGAR, P.C.

/s/ Jordan K. Cameron
Evan A. Schmutz
Jordan K. Cameron
Attorneys for Plaintiff